Hailey CE Primary School

New Technologies Policy

Part A:
E-Safety Policy, incorporating mobile phone/camera policy

Part B:
School ICT Protocols, incorporating Curriculum and Health & Safety matters

Date:

Signed:

Review Date:

Part A:
E-Safety Policy, incorporating mobile phone/camera policy

Development / Monitoring / Review of this Policy

This e-safety policy has been developed by working with:

- Headteacher
- Staff
- Governors
- Parents and Carers

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule for Development / Monitoring / Review

This e-safety policy was approved by the Governing Body on:	
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity
- Surveys / questionnaires of
  - pupils
  - parents / carers
  - staff

Scope of the Policy

This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of the school. In addition, it covers the school's policy on the use of personal mobile phone, camera and similar technologies whilst on school premises or during school-associated events or visits at other sites.

The Education and Inspections Act 2006 empowers Headteachers (to such extent as is reasonable), to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

The policy also indicates what action should be taken by the Headteacher and governing body of the school in the event of any breach of the policy content by an adult – staff, volunteers, parents/carers, visitors or other community users of the school premises.

Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. The school governor lead for safeguarding matters has taken on the responsibilities of E-Safety Governor. The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Co-ordinator / Officer (Headteacher)

Headteacher / Principal and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community.
- The Headteacher and (at least) another member of the Senior Leadership Team / Senior Management Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see flow chart on dealing with e-safety incidents – "Responding to incidents of misuse" and relevant Local Authority HR disciplinary procedures).
- The Headteacher/Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles
- The Headteacher will receive regular monitoring reports from the ICT Technician and other staff as delegated.
- The Headteacher, or member of the senior leadership team will take action as necessary under this policy and under the school's antibullying and behaviour policies as necessary.

E-Safety Coordinator / Officer: Headteacher

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with school technical staff
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments
- meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed

Network Manager / Technical staff: 2014 – 15 Turn it On

Turn it On and any third party security advisors are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required e-safety technical requirements and any Local Authority Guidance that may apply.
- the filtering policy (if it has one), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant

- that the use of the network / internet / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies

Teaching and Support Staff, Volunteers and Governors

are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP)
- they report any suspected misuse or problem to the Headteacher for investigation / action / sanction
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the e-safety and acceptable use policies
- they monitor the use of digital technologies, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Child Protection / Safeguarding Designated Person / Officer

should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow these guidelines on the appropriate use of:

- digital and video images taken at school events
- not using mobile phone or camera technologies whilst on school premises or take images of members of the school pupil or staff community on school premises outside of advertised school events
- supporting their own and their child's adherence to the AUPs they have signed

Policy Statements

Education – pupils

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum should be provided as part of Computing and PHSCE and should be regularly revisited
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and learning activities
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Education – parents / carers

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site
- Parents / Carers evenings / sessions
- High profile events / campaigns eg Safer Internet Day
- Reference to the relevant web sites / publications eg www.swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers (see appendix for further links / resources)

Education & Training – Staff / Volunteers

It is essential that all staff (including short term/supply staff and volunteers) receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.
- The Headteacher in role as e-safety lead will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.
- The Headteacher in role as e-safety lead will provide advice / guidance / training to individuals as required.

Training – Governors

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any relevant sub-committee or involved in child protection. Training will be offered as follows:

- Participation in school training / information sessions for staff or parents
- Attendance at Local Authority and other relevant training events

Technical System Management

School technical systems will be managed in ways that ensure that the school / academy meets recommended technical requirements (these may be outlined in Local Authority policy and guidance). The School's IT supplier and any third party security advisors are responsible for ensuring:

- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users (at KS2 and above) will be provided with a username and secure password. Users are responsible for the security of their username and password and will be required to change their password every year in September.
- The "master / administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher and kept in a secure place (eg school safe)
- Software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.

It should be noted that:

- This policy defines the extent of personal use that users (staff / students / pupils / community users) are allowed on school devices that may be used out of school.
- This policy indicates the terms of when and what executable files staff may download and install on school devices.
- This policy defines the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Bring Your Own Device (BYOD)

Applies to adults working in the school.

- The school has a set of clear expectations and responsibilities for all users
- The school adheres to the Data Protection Act principles
- All users are provided with and accept the Acceptable Use Agreement
- All network systems are secure and access for users is differentiated
- Where possible these devices will be covered by the school's / academy's normal filtering systems, while being used on the premises
- All users will use their username and password and keep this safe
- Mandatory training is undertaken for all staff
- Regular audits and monitoring of usage will take place to ensure compliance
- Any device loss, theft, change of ownership of the device will be reported immediately to the head teacher or their representative.

Homeworking Policy

Hailey School has a Homeworking policy. Any member of staff working from home are subject to the terms of this policy whilst on school business.

Use of digital and video images

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students / pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Students / pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Students' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website
- Student's / Pupil's work can only be published with the permission of the student / pupil and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed / identified - the data protection officer is a member of the admin team.
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data (see Part B of this policy)

- There is an understood procedure for reporting, logging, managing and recovering from information risk incidents ie the head teacher is informed immediately and (s)he implements measures as per Part B of this policy
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office. (see Part B of this policy)

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff / adults working at the school			Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Not Allowed	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission
Mobile phones and similar technologies may be brought to school *(if stored securely and only used in the staff room or offices)*	√			√			
Use of mobile phones in social time (*breaktime, lunch time, and outside of designated hours)*		√		√			
Taking photos on own mobile phones /own cameras			√	√			

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (eg by remote access).
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

- Any digital communication between staff and pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class / group email addresses may be used at KS1, while students / pupils at KS2 and above may be provided with individual school / academy email addresses for educational use.
- Pupils should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff and governors should ensure that:

- No reference should be made in social media to pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The school's use of social media for professional purposes will be checked regularly by the senior risk officer and e-safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

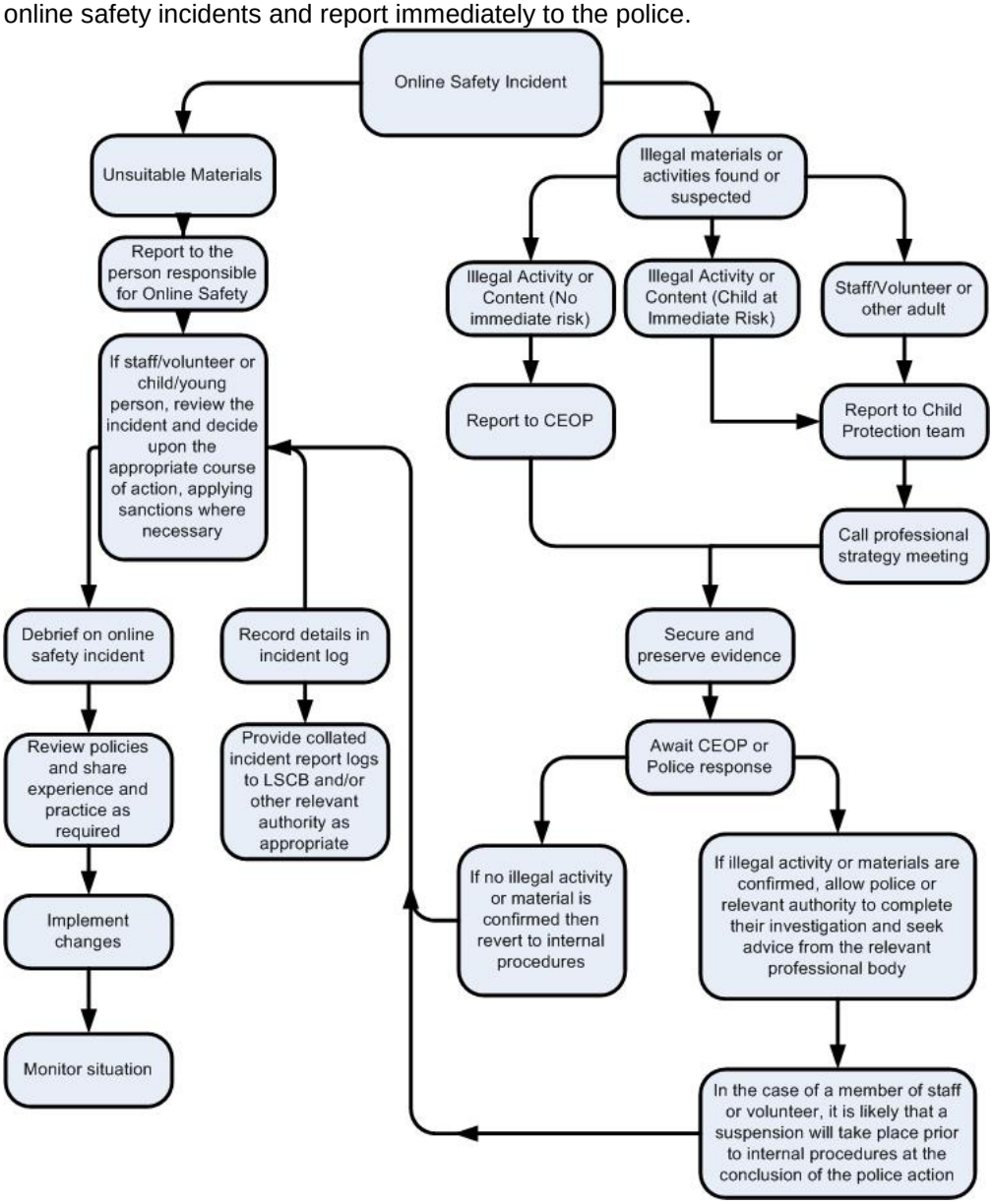
Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978**					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	
On-line gaming (educational) e.g. Abacus, Maths Zone, etc (by staff for lesson planning and by pupils when instructed to do so by a member of staff)			X			
On-line gaming (non educational)					X	
On-line gambling					X	
On-line shopping / commerce (staff members and adult volunteers/governors only; as part of their role or outside of designated hours)			X	X		
File sharing i.e. documents or photos and similar (by pupils or parents/carers at member of staff request only; by staff members/adult volunteers and governors on school business only)			X	X		
Use of social media					**X**	
Use of messaging apps e.g. in case of emergency			**X**	**X**		
Use of video broadcasting eg Youtube (viewing of such for educational purposes only by members of staff or volunteers/governors; pupils viewing of such for educational purposes under supervision of member of staff; posting of material on such sites prohibited for all unless authorised by head teacher)			**X**	**X**		

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the

machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)

- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
  - Internal response or discipline procedures
  - Involvement by Local Authority or national / local organisation (as relevant).
  - Police involvement and/or action
- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
  - incidents of 'grooming' behaviour
  - the sending of obscene materials to a child
  - adult material which potentially breaches the Obscene Publications Act
  - criminally racist material
  - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions For Students/Pupils

Each of the types of incidents listed below will be dealt with on an individual basis and any of the listed sanctions or actions may be used to resolve the matter. Anything illegal shall be automatically referred to the police. The schools behaviour and anti-bullying and equality policies also apply as well as individual pupil circumstances. Patterns or repeated breaches by individuals will incur more severe sanctions.

Incident Type

Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).
Unauthorised use of non-educational sites during lessons
Unauthorised use of mobile phone / digital camera / other mobile device
Unauthorised use of social media / messaging apps / personal email
Unauthorised downloading or uploading of files
Allowing others to access school / academy network by sharing username and passwords
Attempting to access or accessing the school / academy network, using another student's / pupil's account
Attempting to access or accessing the school / academy network, using the account of a member of staff
Corrupting or destroying the data of other users
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature
Continued infringements of the above, following previous warnings or sanctions
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school
Using proxy sites or other means to subvert the school's / academy's filtering system
Accidentally accessing offensive or pornographic material and failing to report the incident
Deliberately accessing or trying to access offensive or pornographic material
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act

Sanction/Action

Refer to class teacher
Refer to Headteacher
Refer to Police
Refer to technical support staff for action re filtering / security etc
Inform parents / carers
Removal of network / internet access rights
Warning
Further sanction eg detention / exclusion

School Actions & Sanctions For Staff/Governors or Volunteers working at the school

Each of the listed types of incidents will be dealt with on an individual basis and any of the listed sanctions or actions may be used to resolve the matter. Anything illegal shall be automatically referred to the police. The schools dignity at work, whistleblowing, behaviour code of conduct, safeguarding, and equality policies apply. The nature of the intent and the consequences of the incident will be considered. Patterns or repeated breaches by individuals will incur more severe sanctions.

Incident Type

Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).
Inappropriate personal use of the internet / social media / personal email
Unauthorised downloading or uploading of files
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account
Careless use of personal data eg holding or transferring data in an insecure manner
Deliberate actions to breach data protection or network security rules
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with pupils
Actions which could compromise the staff member's professional standing
Actions which could bring the school / academy into disrepute or breach the integrity of the ethos of the school
Using proxy sites or other means to subvert the school's filtering system
Accidentally accessing offensive or pornographic material and failing to report the incident
Deliberately accessing or trying to access offensive or pornographic material
Breaching copyright or licensing regulations
Continued infringements of the above, following previous warnings or sanctions

Actions/Sanctions

Refer to line manager
Refer to Headteacher
Refer to Local Authority / HR
Refer to Police
Refer to Technical Support Staff for action re filtering etc
Warning
Suspension
Disciplinary Action

Appendix 1

Pupil Acceptable Use Agreement – for KS2 Pupils

These rules will keep me safe and help me to be fair to others.

I will only use the school's computers for schoolwork and homework.

I will only edit or delete my own files and not look at, or change, other people's files without their permission.

I will keep my logins and passwords secret.

I will not bring files into school without permission or upload inappropriate material to my workspace.

I am aware that some websites and social networks have age restrictions and I should respect this.

I will not attempt to visit internet sites that I know to be banned by the school.

I will only e-mail people I know, or a responsible adult has approved.

The messages I send, or information I upload, will always be polite and sensible.

I will not open an attachment, or download a file, unless I know and trust the person who has sent it.

I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission. I will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.

If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher/responsible adult.

Signed (child):……

Signed (parent): ……..

This AUP is based on one recommended by the London Grid for Learning, produced by Deneholm Primary School, Grays, Essex.

Appendix 2

Pupil Acceptable Use Policy Agreement – for Foundation/KS1 Pupils

This is how we stay safe when we use computers:

I will ask a teacher or suitable adult if I want to use the computers

I will only use activities that a teacher or suitable adult has told or allowed me to use.

I will take care of the computer and other equipment

I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.

I will tell a teacher or suitable adult if I see something that upsets me on the screen.

I know that if I break the rules I might not be allowed to use a computer.

Signed (child):……

Signed (parent): ……..

This AUP is based on one produced by St Mark's Church of England / Methodist Ecumenical VA Primary School, Weston super Mare.

Appendix 3

Parent / Carer Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent / Carers Name | Student / Pupil Name

As the parent / carer of the above students / pupils, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

Either: (KS2)
I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.
Or: (KS1/Foundation Stage)
I understand that the school has discussed the Acceptable Use Agreement with my son / daughter and that they have received, or will receive, e-safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will ensure that my child does not bring a mobile phone, camera, tablet or similar device into school, unless specifically requested by a member of staff.

Apart from at advertised events, I will not use a mobile phone, camera, tablet or similar device on school premises.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Signed | Date

Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media.

The school will comply with the Data Protection Act and request parents / carers permission before taking images of members of the school. We will also ensure that when images are published that the young people can not be identified by the use of their names.

In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act), unless otherwise advised. To respect everyone's privacy and in some cases protection, these images should not be published or made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.

Parents / carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents / carers to agree

Digital / Video Images Permission Form

Parent / Carers Name	
Student / Pupil Name	

As the parent / carer of the above student / pupil, I agree to the school taking and using digital / video images of my child / children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school. Yes / No

I agree to not use mobile phone or camera technologies whilst on the school premises, including to take images of members of the school community (staff or pupil) outside of advertised school events. I agree that if I take digital or video images at, or of, – school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.

Signed	
Date	

Appendix 4

Staff (and Volunteer) Acceptable Use Policy Agreement Template

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools / academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

The school will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, VLE etc) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies (Communications Policy and this E-Safety Policy).
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (PDAs / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems unless for school purposes or outside of designated hours.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in this policy.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the OCC guidelines on Personal Data and data protection legislation). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name

Signed

Date

Appendix 5

Acceptable Use Agreement for Community Users

This Acceptable Use Agreement is intended to ensure:

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential risk in their use of these systems and devices

Acceptable Use Agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school

- I understand that my use of school systems and devices and digital communications will be monitored
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and / or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this Acceptable Use Agreement, the school has the right to remove my access to school systems / devices

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

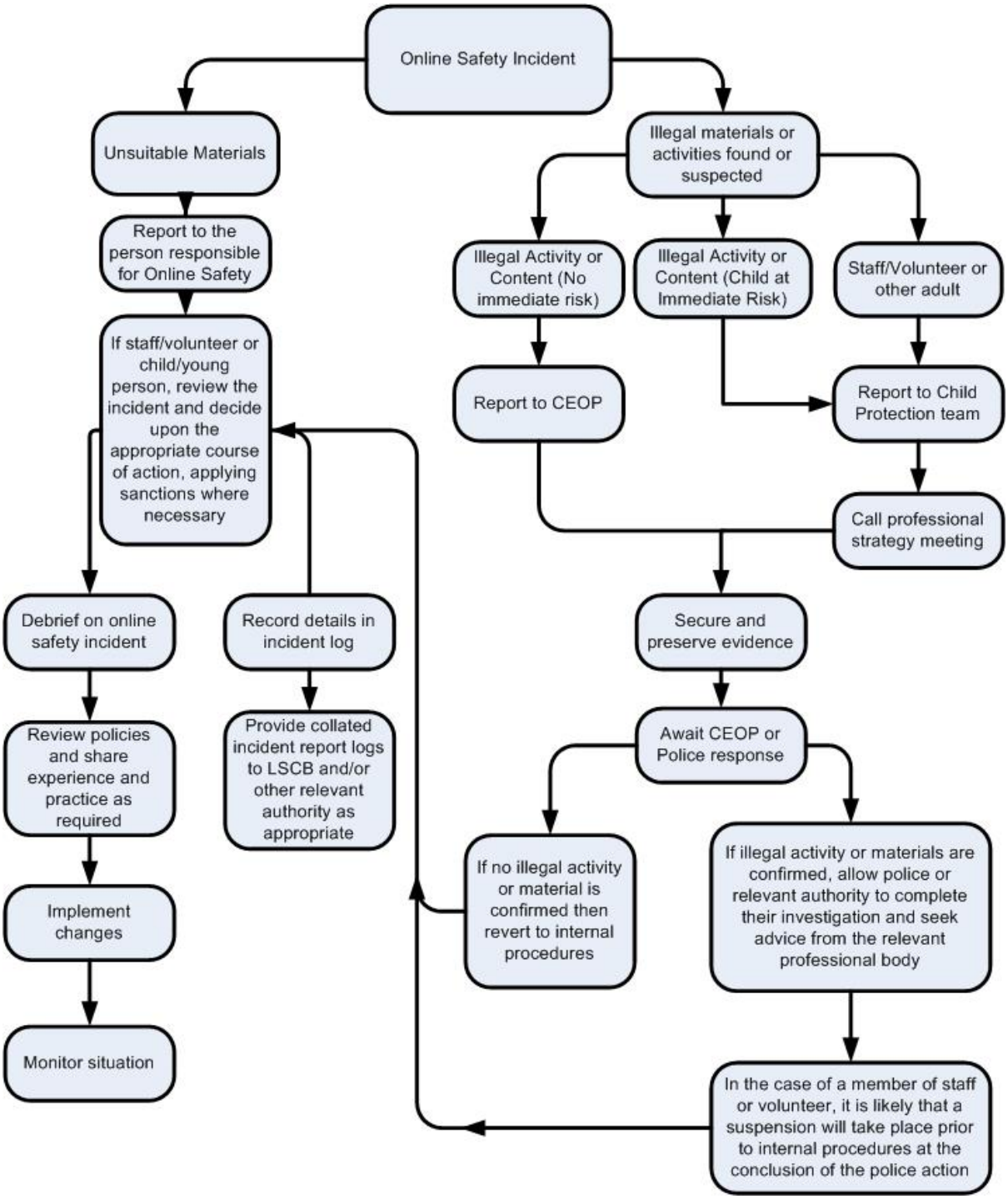
Name

Signed

Date

Appendix 6

Responding to incidents of misuse – flow chart



Appendix 7

Record of reviewing devices / internet sites (responding to incidents of misuse)

Group	
Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

Name and location of computer used for review (for web sites)

Web site(s) address / device	**Reason for concern**

Conclusion and Action proposed or taken

Appendix 8

Template Reporting Log

Reporting Log Group										
Date										
Time										
Incident										
Action taken	What?									
	By whom?									
Incident Reported by										
Signature										

Appendix 9
Training Needs Audit

Training Needs Audit Log
Group ..... Date .....

Name	Position	Relevant training in last 12 months	Identified training need	To be met by:	Cost	Review date

School Technical Security Policy (including filtering and passwords) - amended January 2015

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies).
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school computer systems
- there is oversight from senior leaders and these have impact on policy and practice.

Responsibilities

The management of technical security will be overseen by the Headteacher

Technical Security

Policy statements

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people will receive guidance and training and will be effective in carrying out their responsibilities: (schools will have very different technical infrastructures and differing views as to how these technical issues will be handled – it is therefore essential that this section is fully discussed by a wide range of staff – technical, educational and administrative staff before these statements are agreed and added to the policy:)

- **School technical systems will be managed in ways that ensure that the school meets recommended technical requirements**
- **There will be regular reviews and audits of the safety and security of school technical systems**
- **Servers, wireless systems and cabling must be securely located and physical access restricted**
- **Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.**
- **Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff**.
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The Headteacher is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- An agreed policy is in place for the provision of temporary access of guests eg trainee teachers, supply teachers, visitors onto the school ie guest login created

Password Security

A safe and secure username / password system is essential if the above is to be established and will apply to all school technical systems, including networks, devices and email.

Policy Statements

- All users will have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the E-Safety governor.
- **All school networks and systems will be protected by secure passwords that are regularly changed**
- **The "master / administrator" passwords for the school systems, used by the technical staff must also be available to the Headteacher or other nominated senior leader and kept in a secure place eg school safe.**

Staff passwords:

- **All staff users will be provided with a username and password** by Personnel Administrator who will keep an up to date record of users and their usernames.
- the password should follow industry best practice guidelines for strength
- temporary passwords e.g. used with new user accounts or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on
- passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of school
- should be changed at least every 60 to 90 days
- should not re-used for 6 months and be significantly different from previous passwords; the last four passwords cannot be re-used; passwords should be created by the same user.
- should be different for systems used inside and outside of school

Student / pupil passwords

- Students / pupils will be taught the importance of password security
- The complexity (ie minimum standards) will be set with regards to the cognitive ability of the children.

Training / Awareness

Members of staff will be made aware of the school's password policy:

- at induction
- through the school's e-safety policy and password security policy
- through the Acceptable Use Agreement

Pupils / students will be made aware of the school's password policy:

- in e-safety lessons
- through the Acceptable Use Agreement

Audit / Monitoring / Reporting / Review

The responsible person (Turniton technician in conjunction with the HT) will ensure that full records are kept of:

- User Ids and requests for password changes
- User log-ons
- Security incidents related to this policy

Filtering
Introduction
The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for e-safety and acceptable use. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

Responsibilities
The responsibility for the management of the school's filtering policy will be held by OCC/Turn it On. They will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the school filtering service must:

- **be logged in change control logs**
- **be reported to a second responsible person (Headteacher):**

All users have a responsibility to report immediately to the HT any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Policy Statements
Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the school. Illegal content is filtered by broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the school to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the school network, filtering will be applied that is consistent with school practice.

Education / Training / Awareness
Pupils will be made aware of the importance of filtering systems through the e-safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through: (amend as relevant)

- the Acceptable Use Agreement

Parents will be informed of the school's filtering policy through the Acceptable Use Agreement and through e-safety awareness sessions / newsletter etc.

Monitoring
As well as the OCC filtering system the school will be using Securus from February 2015.

School Personal Data Handling Policy

Policy Statements
The school will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.

Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".

Personal Data

The school and individuals will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the school community – including pupils, members of staff and parents / carers eg names, addresses, contact details, legal guardianship contact details, health records, disciplinary records
- Curricular / academic data eg class lists, pupil / student progress records, reports, references
- Professional records eg employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members.

Responsibilities

The school's data protection officer is a member of the admin team. This person will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the school's information risk policy and risk assessment
- appoint the Information Asset Owners (IAOs) (usually members of the admin team)

The school will identify Information Asset Owners (IAOs) for the various types of data being held (eg pupil / student information / staff information / assessment data etc). The IAOs will manage and address risks to the information and will understand :

- what information is held, for how long and for what purpose,
- how information as been amended or added to over time, and
- who has access to protected data and why.

Everyone in the school has the responsibility of handling protected or sensitive data in a safe and secure manner.

Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

Registration

The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner.

Information to Parents / Carers – the "Privacy Notice"

In order to comply with the fair processing requirements of the DPA, the school will inform parents / carers of all pupils / students of the data they collect, process and hold on the pupils / students, the purposes for which the data is held and the third parties (eg LA, DfE, etc) to whom it may be passed. This privacy notice will be passed to parents / carers through the school newsletter annually. Parents / carers of young people who are new to the school will be provided with the privacy notice through a specific letter.

Training & awareness

All staff will receive data handling awareness / data protection training and will be made aware of their responsibilities, as described in this policy through:

- Induction training for new staff

Risk Assessments

Information risk assessments will be carried out by Information Asset Owners to establish the security measures already in place and whether they are the most appropriate and cost effective. The risk assessment will involve:

- Recognising the risks that are present;
- Judging the level of the risks (both the likelihood and consequences); and

- Prioritising the risks.

Risk assessments are an ongoing process and should result in the completion of an Information Risk Actions Form (example below):

Risk ID	Information Asset affected	Information Asset Owner	Protective Marking (Impact Level)	Likelihood	Overall risk level (low, medium, high)	Action(s) to minimise risk

Impact Levels and protective marking

Following incidents involving loss of data, the Government recommends that the Protective Marking Scheme should be used to indicate the sensitivity of data. The Protective Marking Scheme is mapped to Impact Levels as follows:

Government Protective Marking Scheme label	Impact Level (IL)	Applies to schools?
NOT PROTECTIVELY MARKED	0	Will apply in schools
PROTECT	1 or 2	
RESTRICTED	3	
CONFIDENTIAL	4	Will not apply in schools
HIGHLY CONFIDENTIAL	5	
TOP SECRET	6	

The school will ensure that all school staff, independent contractors working for it, and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as Protect, Restricted or higher. Unmarked material is considered 'unclassified'. The term 'UNCLASSIFIED' or 'NON' or 'NOT PROTECTIVELY MARKED' may be used to indicate positively that a protective marking is not needed.

All documents (manual or digital) that contain protected or restricted data will be labelled clearly with the Impact Level shown in the header and the Release and Destruction classification in the footer.

Users must be aware that when data is aggregated the subsequent impact level may be higher than the individual impact levels of the original data. Combining more and more individual data elements together in a report or data view increases the impact of a breach. A breach that puts pupils at serious risk of harm will have a higher impact than a risk that puts them at low risk of harm. Long-term significant damage to anyone's reputation has a higher impact than damage that might cause short-term embarrassment.

Release and destruction markings should be shown in the footer eg. "Securely delete or shred this information when you have finished using it".

Secure Storage of and access to data

The school will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

All users will use strong passwords which must be changed regularly. User passwords must never be shared.

Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data can only be stored on school equipment (this includes computers and portable storage media (where allowed). Private equipment (ie owned by the users) must not be used for the storage of personal data.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected,
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected),
- the device must offer approved virus and malware checking software (memory sticks will not provide this facility, most mobile devices will not offer malware protection), and
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete.

The school has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups. The school has clear policy and procedures for the use of “Cloud Based Storage Systems” (for example dropbox, google apps and google docs) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data.

As a Data Controller, the school is responsible for the security of any data passed to a “third party”. Data Protection clauses will be included in all contracts where data is likely to be passed to a third party.

All paper based Protected and Restricted (or higher) material must be held in lockable storage, whether on or off site.

The school / academy recognises that under Section 7 of the DPA, http://www.legislation.gov.uk/ukpga/1998/29/section/7 data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place to deal with Subject Access Requests i.e. a written request to see all or a part of the personal data held by the data controller in connection with the data subject. Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data.

Secure transfer of data and access out of school

The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location (see earlier section – LA / school policies may forbid such transfer);
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (eg family members) when out of school

- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform;
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location;
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software; and
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority (if relevant) in this event. (nb. to carry encrypted material is illegal in some countries)

Disposal of data

The school will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance, and other media must be shredded, incinerated or otherwise disintegrated for data.

A Destruction Log should be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.

All significant data protection incidents must be reported through the SIRO to the Information Commissioner's Office based upon the local incident handling policy and communication plan.

Use of technologies and Protective Marking

The following provides a useful guide:

	The information	**The technology**	**Notes on Protect Markings (Impact Level)**
School life and events	School terms, holidays, training days, the curriculum, extra-curricular activities, events, displays of pupils work, lunchtime menus, extended services, parent consultation events	Common practice is to use publically accessible technology such as school websites or portal, emailed newsletters, subscription text services	Most of this information will fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.
Learning and achievement	Individual pupil / student academic, social and behavioural achievements, progress with learning, learning behaviour, how parents can support their child's learning, assessments, attainment, attendance, individual and personalised curriculum and educational needs.	Typically schools will make information available by parents logging on to a system that provides them with appropriately secure access, such as a Learning Platform or portal, or by communication to a personal device or email account belonging to the parent.	Most of this information will fall into the PROTECT (Impact Level 2) category. There may be students/ pupils whose personal data requires a RESTRICTED marking (Impact Level 3) or higher. For example, the home address of a child at risk. In this case, the school may decide not to make this pupil / student record available in this way.
Messages and alerts	Attendance, behavioural, achievement, sickness, school closure, transport arrangements, and other information that it may be important to inform or contact a parent about as soon as possible. This may be particularly important when it is necessary to contact a parent concerning information that may be considered too sensitive to make available using other online means.	Email and text messaging are commonly used by schools to contact and keep parents informed. Where parents are frequently accessing information online then systems e.g. Learning Platforms or portals, might be used to alert parents to issues via "dashboards" of information, or be used to provide further detail and context.	Most of this information will fall into the PROTECT (Impact Level 1) category. However, since it is not practical to encrypt email or text messages to parents, schools should not send detailed personally identifiable information. General, anonymous alerts about schools closures or transport arrangements would fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category.

Appendix 10
DfE Guidance on the wording of the Privacy Notice

PRIVACY NOTICE
for
Pupils in Schools at Hailey CE Primary School

Privacy Notice - Data Protection Act 1998

We **Hailey CE Primary School** are a data controller for the purposes of the Data Protection Act. We collect information from you and may receive information about you from your previous school and the Learning Records Service. We hold this personal data and use it to:

- Support your teaching and learning;
- Monitor and report on your progress;
- Provide appropriate pastoral care, and
- Assess how well your school is doing.

This information includes your contact details, national curriculum assessment results, attendance information and personal characteristics such as your ethnic group, any special educational needs and relevant medical information..

We will not give information about you to anyone outside the school without your consent unless the law and our rules allow us to.

We are required by law to pass some information about you to the Local Authority and the Department for Education (DfE)

If you want to see a copy of the information about you that we hold and/or share, please contact the school office.

If you require more information about how the Local Authority (LA) and/or DfE store and use your information, then please go to the following website:

http://www.education.gov.uk/researchandstatistics/datatdatam/b00212337/datause

If you are unable to access these website we can send you a copy of this information. Please contact the DfE as follows:

Public Communications Unit, Department for Education
Sanctuary Buildings, Great Smith Street, London
SW1P 3BT
Website: www.education.gov.uk
email: http://www.education.gov.uk/help/contactus
Telephone: 0370 000 2288

Appendix 11

Legislation

Schools should be aware of the legislative framework under which this E-Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990
Data Protection Act 1998
Freedom of Information Act 2000
Communications Act 2003
Malicious Communications Act 1988
Regulation of Investigatory Powers Act 2000
Trade Marks Act 1994
Copyright, Designs and Patents Act 1988
Telecommunications Act 1984
Criminal Justice & Public Order Act 1994
Racial and Religious Hatred Act 2006
Protection from Harrassment Act 1997
Protection of Children Act 1978
Sexual Offences Act 2003
Public Order Act 1986
Obscene Publications Act 1959 and 1964
Human Rights Act 1998
The Education and Inspections Act 2006
The Protection of Freedoms Act 2012
The School Information Regulations 2012

Part B:
School ICT Protocols, incorporating Curriculum and Health & Safety matters

Leadership and management

The Vision

We see ICT as an important tool to help bring our children's learning to life;
• to enhance the experiences that are possible as we learn,
• to extend learning and experiences out beyond our school,
• as a communication tool for communication between all members of our community and those outside it.

Review

These protocols are reviewed annually or more often if significant changes in technology arise and all revisions are ratified as delegated by the governing body.

Our strategy to deliver achieve the vision

Day to day responsibility for the delivery of the ICT curriculum rests with class teachers.

The Head Teacher acts as our ICT coordinator and is responsible for developing the school strategy for ICT taking into account opinions expressed by all members of the school community, particularly classroom based staff. This development is also informed by external factors and developments in technology. The Head Teacher is supported by an ICT Lead Governor.

The school maintains an on-going relationship with Turn It On for ICT Support and we seek to ensure that, where appropriate, our ICT development reflect priorities at local authority and national levels. The recommendations of our technical support provider are also taken very seriously.

Environmental impact

Our school takes seriously all issues relating to the environment and this is no less true with ICT. We strive to ensure that all purchasing decisions are backed by sound research and guidance so that every piece of ICT equipment will last as long as possible.

With the assistance of our technical support providers we strive to ensure that the life of any piece of ICT equipment is extended as long as is reasonably possible without making unnecessary demands on technical support or causing unnecessary problems in lessons.

At the end of their useful life we ensure that computer equipment is disposed of in an environmentally friendly way, safely and securely, after any data has been removed.

Health and Safety

Pupils are encouraged from the earliest age to consider and adjust their posture when using the keyboard in order to avoid strain to the arms and back. Hailey School has current policies on safe posture and display screen usage and staff are provided with appropriate training according to these guidelines.

Staff should consult the SENCO and CSTs with regard to any implications of the use of ICT for known medical conditions e.g epilepsy, visual impairment.

Staff using digital projectors should be made aware of the safety guidelines and follow the safety guidelines in them.

Equality

All pupils should develop positive attitudes towards ICT, they should develop an understanding of the potential of ICT and show confidence and enjoyment in its use.

Hailey School ensures that there is equality of access and quality of experience for all pupils according to need and irrespective of race, gender, disability, age and class. Those who are most proficient with the technology will be encouraged to share their expertise and confidence.

Pupils who experience difficulty with mastering the technology or just work more slowly should be allowed extra time or opportunities to work with ICT. Specialised access software and hardware will be available for pupils with special educational needs. All reviews of provision for pupils with special needs should include consideration of a child's access to a computer. Consideration should be given to the most appropriate input device for all pupils but especially those with special needs.

Safeguarding

The school has a specific policy on E-Safety. Please see Part A of this document.

Communication strategy

Our school website www.hailey.oxon.sch.uk is used primarily as a window on our school for those that are not already a part of our community.

Our website is hosted by WebFaction and managed on a day to day basis by our school admin staff with support from our ICT Lead Governor. Class teachers regularly contribute to their class pages to communicate to parents the work of their children.

School planning for ICT

Our school plans and delivers ICT both as a discrete subject and across the curriculum. All planning for ICT begins with the whole curriculum and teachers plan ICT opportunities where they will enhance, extend and motivate learning in other areas.

Our ICT curriculum is based around the three main headings in the Key Stage 1 and 2 programmes of study:

- Exchanging and sharing information
- Finding things out
- Developing ideas and making things happen

ICT does not feature on class time tables; instead it is integrated into other subjects and takes place as indicated in on-going planning.

Planning for continuity within and between classes, phases and schools

The classroom teachers and support staff work with pupils to develop ICT capability. There are well planned ICT and E-safety progressions that allow excellent continuity of experiences and enable staff to build on prior learning in ICT, both in the development of pupils' ICT capability across the curriculum and where pupils use these skills to support learning in other curriculum areas.

The ICT Coordinator will draw on many resources, such as ICT-specific modules and provision in the Cornerstone curriculum the school is adopting, to ensure an engaging programme for our pupils. Samples of planning are reviewed to ensure ICT skills and Knowledge & Understanding are embedded in subject plans and key learning objectives, key skills, assessment etc on discrete progression documents for each year group.

Planning for ICT for inclusion

We recognise the advantages of the using of ICT for pupils with additional needs and we use ICT to:

- address pupils individual needs

• increase access to the curriculum
• improve language skills

We promote equal opportunities for computer usage.

The school monitors the level of access to computers in the home environment to ensure no pupils are unduly disadvantaged. Additional access to computers during school hours is provided for pupils who do not have computers at home.

Computer hardware, software and peripherals used in the school are chosen to ensure that they are non-discriminatory and promote equal opportunities.

All pupils follow the National Curriculum including the development of ICT Capability.

Planning for e-safety

Please see the school E-safety policy.

Curriculum leadership

Leadership is provided by the ICT coordinator who has responsibility for the development of the school's ICT curriculum. The ICT coordinator monitors ICT teaching across the school to help ensure a consistent approach and proper coverage of the curriculum. The ICT coordinator ensures that resources are in place to support this teaching. Where local resources are insufficient or inadequate we actively look for solutions, including collaboration opportunities.

Leadership of learning and teaching with ICT

All class teachers and subject leaders play a role in the development of ICT resources which help to extend and enhance learning within specific subject areas. Discussion takes place on an on-going basis between class teachers and subject leaders with the ICT coordinator as to how resources might best be developed.

Evaluating learning and teaching with ICT

All class teachers are responsible for the on-going evaluation of their own teaching and their children's learning. ICT is heavily linked to learning in all subjects and is therefore constantly under review along with those other subjects.

The ICT coordinator has responsibility for monitoring the teaching of ICT. This is carried out through an examination of:

- Review of teachers' ICT planning
- Review of children's work
- Observations of lessons where ICT capability is being developed.

Where possible, we follow the national ICT curriculum. Further details are available on the school website.

<u>Section 3 Learning</u>

Developing ICT capability
Our planned curriculum includes opportunities for children to develop their ICT capability. Teachers need to be clear about what the learning objectives are to develop that capability, and assess children's progress in learning techniques, applying these techniques in their learning and in developing their higher order thinking making qualitative judgements about when and when not to use ICT.

ICT use for learning and teaching
In addition, children make use of ICT to enhance their learning across the curriculum regardless of whether the activity helps develop ICT capability. A range of digital learning resources are available in and out of school for this purpose (see section 6 of this policy).

Learning with ICT beyond the school

All children are encouraged to make use of ICT outside school. Homework which specifically makes us of ICT is set from time to time, for example “Bug Club”. Children are encouraged to make use of their own ICT facilities at home to complete home based tasks.

Section 4 Assessment of ICT capability

Assessment, recording and reporting of ICT capability

We recognise that assessment is central to classroom practice. Effective assessment establishes what a child knows, understands and can do. It also informs the planning of future learning and enables a school to review the effectiveness of the curriculum and teaching. All teachers report annually to parents, describing progress in ICT. This report contains comments on the child's progress, achievement, strengths, weaknesses and next steps.

Section 5 Professional development

Planning for professional development

Individual development needs are identified by the ICT coordinator on an on-going basis. The evaluation of ICT teaching and learning is also used to identify gaps in individual teachers’ knowledge. All teachers are encouraged to identify specific ICT skill needs in the performance management process.

Identifying whole school ICT development needs

Whole school development needs are often associated with the introduction of technology new to the school, or with the development of already existing resources. These needs are considered at the point of introducing technology and training and support should be built into school’s professional development plans.

Implementation

The ICT coordinator considers the needs of individual members of staff and the school as a whole and provides appropriate support. This support may be provided

- internally (using skills already in the school) via coaching, mentoring and sharing of skills
- by the school’s ICT support provider
- by collaboration, e.g. a teacher in another school
- externally by third party providers of support / suppliers of equipment

Support may be in a variety of forms as appropriate:

- whole school staff meeting
- individual support for teachers
- in class support for teachers alongside the children
- attendance at an appropriate course
- by using appropriate e-learning resources

Review

The ICT coordinator monitors the impact of professional development activities with due regard for the effect on learning and teaching and with “value for money” in mind. Future professional development and performance management reviews build on the results of this evaluation of support provided.

We recognise that ICT capability is best developed when there is a real reason both to develop and apply the particular aspect of ICT and when children have access to resources as a normal part of their learning. For this reason we endeavour to ensure that ICT resources are as accessible to children as possible in their normal learning environment.

Each member of staff is allocated a laptop for school use while they are employed by our school. This is for professional use and is used as indicated in the school’s E-safety policy.

All members of our school community sign acceptable use agreements before they are permitted to use any ICT facilities (see E-safety policy).

Environments for online learning

Our school has taken the decision not to use a formal VLE. Instead we use more limited facility on our school website to share information with parents and to point children in the direction of appropriate online learning experiences linked to our curriculum.

Management information systems (SIMS)
SIMS is used as our core school information management system by staff in terms of attendance. Hailey uses its own data management for assessment and data analysis purposes.

Our resident on-site expert is our ICT Lead Governor and we are supported by contracted ICT support provider Turn It On.

Management of ICT resources
All procurement decisions are informed by the learning and teaching agenda. We make use of collaboration opportunities if available to achieve best value with procurement. We endeavour to take into account the total cost of ownership when making procurement decisions.

Purchasing decisions are made after consultation with our technical support provider (Turn it On) and following both school and local authority procurement guidelines and policy.

No equipment is connected to our network unless it has been approved by our technical support provider.

Software licenses and on-line content subscriptions are often purchased, where possible, through local authority bulk purchasing arrangements to achieve substantial discounts.

Every effort is made to ensure that equipment is disposed of safely and in an environmentally friendly way at the end of its useful life. (see section 1b above)

Technical support
We receive technical support from Turn It On; the precise nature of the support we receive can be found in the support level agreement.

Urgent issues are reported to the ICT coordinator who communicates them to our technical support service directly, or by deputising to a member of the office staff. In such cases problems are solved either remotely or with an additional visit.

Our technical support provider is well placed to hold conversations with all providers of ICT solutions to the school and is usually able to solve any issues.

Our allocated ICT Engineer, together with the ICT coordinator, constantly monitors the effectiveness of solutions and advises on further development and replacement.

Data security and safeguarding
Please see the school's E-safety policy.

Data recovery and risk management
Our systems and processes are regularly reviewed to assess the security of our data and the school's resilience to loss of equipment by theft, fire or hardware failure. All electronic data is either hosted on remote, secure networks or backed up to remote, secure locations.